

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-165378

(43)Date of publication of application : 16.06.2000

(51)Int. Cl.

H04L 9/32

G06T 7/00

G09C 1/00

H04L 9/08

(21)Application number : 10-335723

(71)Applicant : KODO IDO TSUSHIN SECURITY GIJUTSU
KENKYUSHO:KK

(22)Date of filing : 26.11.1998

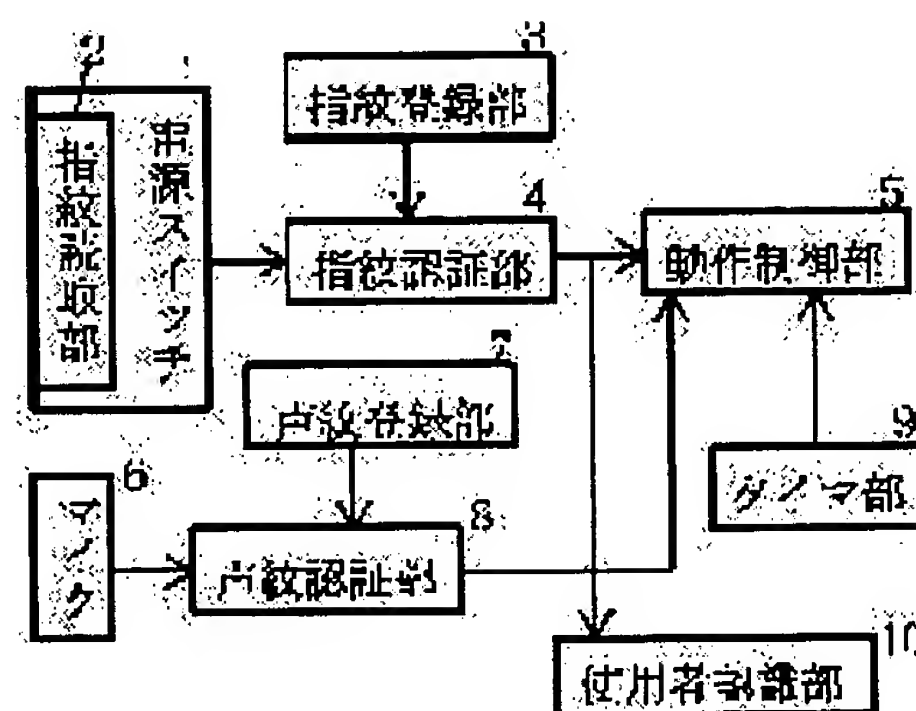
(72)Inventor : ANZAI JUN
KATO TAKEHIKO
MATSUZAKI NATSUME
ITO SATORU

(54) FINGERPRINT AUTHENTICATION DEVICE

(57)Abstract:

PROBLEM TO BE SOLVED: To enhance security of a mobile radio terminal or the like by authenticating a fingerprint with a simple operation.

SOLUTION: A power switch 1 of a mobile radio terminal is provided with a fingerprint read section 2. When the power switch 1 is depressed, a fingerprint is authenticated and when the fingerprint is coincident with a fingerprint registered in a fingerprint registration section 3, the mobile radio terminal can be operated. Furthermore, a voiceprint picked up by a microphone 6 is collated with a voiceprint registered in a voiceprint registration section 7 and when they are coincident, a speech is made available. When a prescribed time elapses after the start of speech, a timer section 9 turns off the power. Even when the terminal in an operating state is missing or stolen, illegal use of the terminal can be prevented. The fingerprint can be authenticated with a simple operation of depression of the switch 1, and the security of the mobile terminal is enhanced. Or a multi-stage switch is used for a speech switch, it is configured such that half-depression causes fingerprint authentication and full-depression starts a speech.



LEGAL STATUS

[Date of request for examination]

02.06.1999

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

3258632

[Date of registration]

07.12.2001

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

・[Date of extinction of right]

Copyright (C); 1998, 2003 Japan Patent Office

* NOTICES *

Japan Patent Office is not responsible for any damages caused by the use of this translation.

1. This document has been translated by computer. So the translation may not reflect the original precisely.
2. **** shows the word which can not be translated.
3. In the drawings, any words are not translated.

CLAIMS

(57) [Claim(s)]

[Claim 1] Fingerprint authentication equipment characterized by providing the following. The fingerprint read station prepared in the electric power switch or the switch of operation of electronic equipment. The fingerprint registration section which can register two or more men's fingerprint. The fingerprint authentication section which compares the reading fingerprint data and the registration fingerprint data of the aforementioned fingerprint registration section which were read by the aforementioned fingerprint read station. A means to operate the aforementioned electronic equipment based on the comparison result of the aforementioned fingerprint authentication section, The means which will turn OFF a power supply if the aforementioned electronic equipment carries out after [a start of operation] fixed time progress, the difference of a means to recognize the person registered into the fingerprint registration section as a person who used the aforementioned electronic equipment based on the comparison result of the aforementioned fingerprint authentication section, and the aforementioned registration fingerprint data and the aforementioned reading fingerprint data -- a means to ask for data, and the above -- difference -- a means to generate a random number based on data

[Claim 2] Fingerprint authentication equipment according to claim 1 characterized by establishing a means to attest a partner's digital signature while generating a digital signature using the aforementioned random number. [Claim 3] Fingerprint authentication equipment according to claim 1 characterized by establishing a means to perform key share processing using the aforementioned random number. [Claim 4] Fingerprint authentication equipment according to claim 1 characterized by establishing a means to perform encryption processing by public key encryption using the aforementioned random number. [Claim 5] Fingerprint authentication equipment according to claim 1 which considers the aforementioned telephone call switch as a multi-stage switch, and is characterized by establishing fingerprint authentication, a means to perform random number generation, and the means that enables communication of the aforementioned mobile radio terminal based on the result of fingerprint authentication in all the push states of the aforementioned telephone call switch in the half-push state of the aforementioned telephone call switch.

[Translation done.]

* NOTICES *

Japan Patent Office is not responsible for any damages caused by the use of this translation.

1. This document has been translated by computer. So the translation may not reflect the original precisely.
2. **** shows the word which can not be translated.
3. In the drawings, any words are not translated.

DETAILED DESCRIPTION

[Detailed Description of the Invention]

[0001]

[The technical field to which invention belongs] this invention relates to the fingerprint authentication equipment which generates a random number especially based on a user's fingerprint about the fingerprint authentication equipment used for a mobile radio terminal etc.

[0002]

[Description of the Prior Art] After conventional fingerprint authentication equipment turns on the electric power switch of a device, a finger is applied to fingerprint authentication equipment, fingerprint authentication is performed, and if authentication is passed, a device will operate. Or the electric power switch of a device is always turned on [it], if fingerprint authentication is passed, a switch of operation will become effective and a device will operate.

[0003] The radio terminal as shown in drawing 3 is indicated by JP,10-51441,A. This is a radio terminal which has the advanced security function which cannot always perform a user's fingerprint collating during use, and only the specified user can use. The fingerprint of the finger which pushed the communication button is incorporated as a user fingerprint in the fingerprint taking-in section, this user fingerprint is collated with a registration fingerprint in the fingerprint discernment section, and it discriminates [coincidence or] whether it is inharmonious. A communication switch detects that the communication button is pushed and communication is made possible a condition [this]. When a registration fingerprint and a user fingerprint are inharmonious, the communications department ends communication.

[0004] The portable telephone is indicated by JP,6-284182,A. This is the radio formula portable telephone which the person who gathered can connect to an original user easily, when sufficient security function make it not make men other than an original user use is had and dropped. A security control section controls the fingerprint reading section, the fingerprint registration section, a fingerprint collating comparator, and the fingerprint temporary storage section, and makes registration of a fingerprint, and collating perform according to operation of a security button and an electric power switch, and performs the change of a security state and a security release state. Moreover, whenever the button for an emergency call is pushed, in two or more emergency call places, emergency call control means switch the emergency call place which carries out call origination to the high order of priority, display an emergency call place on a display, control a telephone function part, and it carries out call origination to the telephone number of the emergency call place read from the telephone number storage section for an emergency call.

[0005] Cellular-phone equipment is indicated by JP,5-95329,A. As compared with the information which read a specific user's human body-information (fingerprint) by the fingerprint read station, and memorized it beforehand, this is cellular-phone equipment which makes the transceiver section operating state, when in agreement. A vocal parameter can also be compared instead of a fingerprint.

[0006] The personal computer system is indicated by JP,10-1984453,A. Replace a password input with fingerprint collating and a substantial security function is aimed at, and also this is carrying a finger sensor in a system, and automation of an environmental setup by the user individual etc. is the personal computer system which realized the high usage of versatility. The finger data extracted by the finger sensor are incorporated to a system, the environmental setting data defined are generated the whole finger data, and it registers as a database (finger registration environmental setting table), when there is a finger entry of data, comparison collating with a database is performed, and automatic setup operation is carried out according to the environmental setting information registered by the result of the comparison collating.

[0007]

[Problem(s) to be Solved by the Invention] However, with conventional equipment, it is only attesting an individual by fingerprint collating, and fingerprint data were not utilized enough. Therefore, since the method of raising security using many equipments had to be taken, there was a problem that the cost of equipment became high. Moreover, in the case of a mobile radio terminal, only discernment of the terminal unit itself was completed but there were who a user's being and a problem of not being discriminable.

[0008] Moreover, although the magnetic card is used and management which is charged for every section using an authentication result was performed by electronic equipment other than a mobile radio terminal, for example, a copy machine, in order to attest a user, there was a problem that it was difficult to prevent the unauthorized use by loss, unapproved borrowing, etc. of a magnetic card.

[0009] this invention solves the above-mentioned conventional problem, and aims at curtailment of the step accompanying the improvement in security and it by fingerprint authentication.

[0010] Moreover, the user of electronic equipment is managed with a fingerprint and it aims at enabling it to charge a copy machine etc. for every section.

[0011]

[Means for Solving the Problem] The fingerprint read station which formed fingerprint authentication equipment in the electric power switch or the switch of operation of electronic equipment in this invention in order to solve the above-mentioned technical problem, The fingerprint authentication section which compares the fingerprint registration section which can register two or more men's

fingerprint with the reading fingerprint data and the registration fingerprint data of the fingerprint registration section read by the fingerprint read station, It considered as the composition possessing a means to operate electronic equipment based on the comparison result of the fingerprint authentication section, the means which will turn OFF a power supply if electronic equipment carries out after [a start of operation] fixed time progress, and a means to recognize the person who used electronic equipment. Thus, since starting and operation of are not done unless authentication operation becomes unnecessary and it clears fingerprint authentication, but a power supply ON state also goes out in fixed time by having constituted, while being able to prevent an unauthorized use, it can be used by two or more men of specification [a device], and a device user can be discriminated and displayed.

[0012] Moreover, the fingerprint read station was prepared in the telephone call switch of a mobile radio terminal. Thus, by having constituted, if authentication operation becomes unnecessary and fingerprint authentication is not cleared, it cannot talk over the telephone at a mobile radio terminal, but an unauthorized use can be prevented.

[0013] Moreover, the voiceprint authentication section which compares the voiceprint registration section which registers people's voiceprint with the audio input voiceprint data and the registration voiceprint data of the voiceprint registration section inputted into the transmission microphone, and performs voiceprint authentication, and the means which enables communication of a mobile radio terminal based on the result of voiceprint authentication were established. Thus, by having constituted, if authentication operation becomes unnecessary and voiceprint authentication is not cleared, either, it cannot talk over the telephone at a mobile radio terminal, but an unauthorized use can be prevented.

[0014] Moreover, the fingerprint read station was prepared in the copy switch of a copying machine. Thus, by having constituted, if authentication operation becomes unnecessary and fingerprint authentication is not cleared, a copying machine cannot copy but an unauthorized use can be prevented.

[0015] moreover, the difference of registration fingerprint data and reading fingerprint data -- a means to ask for data, and difference - a means to generate a random number based on data was established Thus, by having constituted, a random number is easily generable.

[0016] Moreover, while generating the digital signature using the random number, a means to attest a partner's digital signature was established. Thus, by having constituted, a digital signature and partner authentication can be performed efficiently.

[0017] Moreover, a means to perform key share processing using a random number was established. Thus, by having constituted, a key share can be performed efficiently.

[0018] Moreover, a means to perform encryption processing by public key encryption using a random number was established. Thus, by having constituted, encryption processing can be performed efficiently.

[0019] Moreover, the telephone call switch was considered as the multi-stage switch, and fingerprint authentication, a means to perform random number generation, and the means that enables communication of a mobile radio terminal based on the result of fingerprint authentication in all the push states of a telephone call switch were established in the half-push state of a telephone call switch. Thus, by having constituted, the function of authentication and a telephone call can be chosen with one switch.

[0020]

[Embodiments of the Invention] The fingerprint read station which prepared invention indicated to the claim 1 of this invention in the electric power switch or the switch of operation of electronic equipment, The fingerprint authentication section which compares the fingerprint registration section which can register two or more men's fingerprint with the reading fingerprint data and the registration fingerprint data of the aforementioned fingerprint registration section read by the aforementioned fingerprint read station, A means to operate the aforementioned electronic equipment based on the comparison result of the aforementioned fingerprint authentication section, The means which will turn OFF a power supply if the aforementioned electronic equipment carries out after [a start of operation] fixed time progress, A means to recognize the person registered into the fingerprint registration section as a person who used the aforementioned electronic equipment based on the comparison result of the aforementioned fingerprint authentication section, the difference of the aforementioned registration fingerprint data and the aforementioned reading fingerprint data -- with a means to ask for data the above -- difference -- it is fingerprint authentication equipment possessing a means to generate a random number based on data, fingerprint authentication is performed at the time of a switch depression, and while restricting operation at fixed time and preventing an unauthorized use, it has operation of generating a random number using the noise component of a fingerprint

[0021] In fingerprint authentication equipment according to claim 1, invention of this invention according to claim 2 establishes a means to attest a partner's digital signature while generating a digital signature using the aforementioned random number, and it has operation of simplifying a digital signature and partner authentication. [0022] In fingerprint authentication equipment according to claim 1, invention of this invention according to claim 3 establishes a means to perform key share processing using the aforementioned random number, and has operation of simplifying key share processing.

[0023] In fingerprint authentication equipment according to claim 1, invention of this invention according to claim 4 establishes a means to perform encryption processing by public key encryption using the aforementioned random number, and has operation of simplifying the encryption processing by public key encryption.

[0024] Invention of this invention according to claim 5 is set to fingerprint authentication equipment according to claim 1. A means to consider the aforementioned telephone call switch as a multi-stage switch, and to perform fingerprint authentication and random number generation in the half-push state of the aforementioned telephone call switch, The means which enables communication of the aforementioned mobile radio terminal based on the result of fingerprint authentication in all the push states of the aforementioned telephone call switch is established, and it has operation of making authentication and random number generation, and a telephone call serve a double purpose with one switch.

[0025]

[0026]

[0027]

[0028]

[0029] Hereafter, the form of operation of this invention is explained in detail, referring to drawing 1 and drawing 2 .

[0030] (Form of the 1st operation) The form of operation of the 1st of this invention Prepare a fingerprint read station in the electric power switch of a mobile radio terminal, and two or more men's fingerprint is registered into the fingerprint registration section. The fingerprint authentication section compares the reading fingerprint data and the registration fingerprint data of the fingerprint registration section which were read by the fingerprint read station. While recognizing a user based on the comparison result of the fingerprint authentication section, a mobile radio terminal is operated. When communication of a mobile radio terminal is enabled based on the result which compared the voiceprint data of input voice with the registered voiceprint data and a mobile radio terminal carries out after [a start of operation] fixed time progress, it is fingerprint authentication equipment which turns OFF a power supply.

[0031] Drawing 1 is the functional block diagram of the fingerprint authentication equipment of the form of operation of the 1st of this invention. In drawing 1 , an electric power switch 1 is an electric power switch of a mobile radio terminal. The fingerprint read station 2 is a means to read a user's fingerprint. The fingerprint registration section 3 is the storage which registered two or more men's fingerprint. The fingerprint authentication section 4 is a means to compare the reading fingerprint data and the registration fingerprint data of the fingerprint registration section 3 which were read by the fingerprint read station 2. The motion-control section 5 is a means to operate a mobile radio terminal based on the comparison result of the fingerprint authentication section 4. A microphone 6 is a microphone for transmission of a mobile radio terminal. The voiceprint registration section 7 is the storage which registered two or more users' voiceprint. The voiceprint authentication section 8 is a means to compare the voiceprint data and registration voiceprint data of input voice, and to perform voiceprint authentication. The timer section 9 is a means which turns OFF a power supply, when a mobile radio terminal carries out after [a start of operation] fixed time progress. The user recognition section 10 is a means to recognize the person who used the mobile radio terminal.

[0032] Operation of the fingerprint authentication equipment of the form of operation of the 1st of this invention constituted as mentioned above is explained.

[0033] A fingerprint is read by the fingerprint read station 2 prepared in the electric power switch 1 of a mobile radio terminal. Two or more men's fingerprint is registered into the fingerprint registration section 3. The fingerprint authentication section 4 compares the reading fingerprint data and the registration fingerprint data of the fingerprint registration section 3 which were read by the fingerprint read station 2. The person who used the mobile radio terminal in the user recognition section 10 according to the fingerprint authentication result is recognized. Although the motion-control section 5 operates a mobile radio terminal based on the comparison result of the fingerprint authentication section 4, it does not still have an end possible [communication].

[0034] Two or more men's voiceprint is registered into the voiceprint registration section 7. The voiceprint authentication section 8 compares the audio input voiceprint data and the registration voiceprint data of the voiceprint registration section 7 which were inputted into the microphone 6, and voiceprint authentication is performed. Communication of a mobile radio terminal is enabled based on the result of voiceprint authentication. It uses together with fingerprint authentication, voiceprint authentication is performed, and security is raised more. By registering two or more fingerprints and voiceprints of people, a mobile radio terminal can be used by two or more men.

[0035] If a mobile radio terminal carries out after [a start of operation] fixed time progress, a power supply will be turned OFF by the timer section 9. Since a power supply is shut off in fixed time by the timer section 9 even if it carries out authentication success and starts, an unauthorized use can be prevented also by loss with operating state, or the case of a theft.

[0036] As mentioned above, with the form of operation of the 1st of this invention, since it considered as the composition which fingerprint authentication equipment is formed for the fingerprint authentication section in the electric power switch of a mobile radio terminal, and a switch and fingerprint authentication are interlocked, and is operated by fingerprint authentication, fingerprint authentication can be performed only in operation of pushing a switch, and security can be raised.

[0037] In addition, although the form of this operation explained what formed fingerprint authentication equipment in the mobile radio terminal, a fingerprint read station can be prepared in the electric power switch or copy switch of a copying machine, and the user of a copying machine can also be limited. Thus, even if it does not use a magnetic card, it can charge for every section, and accounting management can be performed easily and strictly with prevention of an unauthorized use.

[0038] (Form of the 2nd operation) The form of operation of the 2nd of this invention Use a multi-stage switch for a mobile radio terminal, and if it is all push, it will talk over the telephone. It is fingerprint authentication equipment which will perform authentication and random number generation if it is half-push, generates a random number from the difference of the fingerprint recognized to be a registered fingerprint, performs a digital signature and partner authentication using a random number, does key sharing using a random number, and performs encryption by public key encryption using a random number.

[0039] Drawing 2 is the functional block diagram of the fingerprint authentication equipment of the form of operation of the 2nd of this invention. In drawing 2 , it is the multi-stage switch which the telephone call switch 21 performs fingerprint authentication and random number generation in a half-push state, and enables communication of a mobile radio terminal based on the result of fingerprint authentication in all push states. the random number generation section 22 -- the difference of registration fingerprint data and reading fingerprint data -- data -- asking -- difference -- it is a means to generate a random number based on data The digital signature section 23 is a means to attest a partner's digital signature while generating a digital signature using a random number. The key share processing section 24 is a means to perform key share processing using a random number. The encryption processing section 25 is a means to perform encryption processing by public key encryption using a random number.

[0040] Operation of the fingerprint authentication equipment of the form of operation of the 2nd of this invention constituted as mentioned above is explained. In the half-push state of the multi-stage telephone call switch 21 of a mobile radio terminal, fingerprint authentication and random number generation are performed and communication of a mobile radio terminal is enabled in all the push states of the telephone call switch 21 based on the result of fingerprint authentication.

[0041] the random number generation section 22 -- setting -- difference, such as a position of the fingerprint of registration fingerprint data and reading fingerprint data, a range, an angle, and the amount of data, -- data -- asking -- difference -- a random number is generated for data as seed of a pseudo-random number generator In the digital signature section 23, while generating a digital signature using a random number, a partner's digital signature is attested. In the key share processing section 24, key share processing

is performed using a random number. In the encryption processing section 25, encryption processing by public key encryption is performed using a random number. Since the random number is required for an ElGamal signature, a DSA signature, an ellipse ElGamal signature, an ellipse DSA signature, an D-H key share, an ellipse DH key share, an ElGamal code, and an ellipse ElGamal code, generation of a digital signature etc. can be easily performed using the random number for which it asked from fingerprint data. [0042] as mentioned above, with the form of operation of the 2nd of this invention Using a multi-stage switch, fingerprint authentication equipment will be talked over the telephone, if it is all push. Since authentication and random number generation were performed, the random number was generated from the difference of the fingerprint recognized to be a registered fingerprint and it considered as the composition which performs a digital signature and partner authentication, key share, and encryption by public key encryption using the random number when it was half-push Various kinds of cipher processing can be easily performed using the random number generated from the fingerprint.

[0043]

[Effect of the Invention] As mentioned above, the fingerprint read station which formed fingerprint authentication equipment in the electric power switch or the switch of operation of electronic equipment in this invention, The fingerprint authentication section which compares the fingerprint registration section which can register two or more men's fingerprint with the reading fingerprint data and the registration fingerprint data of the fingerprint registration section read by the fingerprint read station, Since it considered as the composition possessing a means to operate electronic equipment based on the comparison result of the fingerprint authentication section, the means which will turn OFF a power supply if electronic equipment carries out after [a start of operation] fixed time progress, and a means to recognize the person who used electronic equipment Fingerprint authentication is carried out by one operation, those who use a terminal can be discriminated and the effect that an unauthorized use can be prevented also by the case of loss or a theft while ** has been operating state is acquired.

[0044] Moreover, since it considered as the composition which the fingerprint authentication section is prepared [composition] in the telephone call switch of a mobile radio terminal, and interlocks a switch and fingerprint authentication, fingerprint authentication is carried out by telephone call switch operation, and the effect that the unauthorized use of a mobile radio terminal can be prevented is acquired.

[0045] Moreover, since the voiceprint authentication section which compares the voiceprint registration section which registers people's voiceprint with the audio input voiceprint data and the registration voiceprint data of the voiceprint registration section inputted into the transmission microphone, and performs voiceprint authentication, and the means which enable communication of a mobile radio terminal based on the result of voiceprint authentication established, the effect that security can raise more is acquired.

[0046] Moreover, since the fingerprint authentication section was prepared in the copy switch of a copying machine, while carrying out fingerprint authentication by operation of a copy switch, interlocking a switch and fingerprint authentication and being able to prevent the unauthorized use of a copying machine, the effect that accounting for every section etc. is made easily is acquired.

[0047] moreover, the difference of registration fingerprint data and reading fingerprint data -- a means to ask for data, and difference - since a means to generate a random number based on data was established, the effect that a random number is easily generable is acquired from the noise component of a fingerprint

[0048] Moreover, since a means to attest a partner's digital signature was established while generating the digital signature using the random number, the effect that a digital signature and partner authentication can be performed simply is acquired from a random number.

[0049] Moreover, since a means to perform key share processing using a random number was established, the effect that key sharing can be done easily is acquired from a random number.

[0050] Moreover, since a means to perform encryption processing by public key encryption using a random number was established, the effect that encryption processing by public key encryption can be performed easily is acquired from a random number.

[0051] Moreover, a telephone call switch considers as a multi-stage switch, and since fingerprint authentication, a means perform random number generation, and the means that enables communication of a mobile radio terminal based on the result of fingerprint authentication in all the push states of a telephone call switch established in the half-push state of a telephone call switch, the effect that authentication and random number generation, and a telephone call can carry out easy is acquired with one switch.

[Translation done.]

* NOTICES *

Japan Patent Office is not responsible for any damages caused by the use of this translation.

1. This document has been translated by computer. So the translation may not reflect the original precisely.
2. **** shows the word which can not be translated.
3. In the drawings, any words are not translated.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]

[Drawing 1] The functional block diagram of the fingerprint authentication equipment of the gestalt of operation of the 1st of this invention,

[Drawing 2] The functional block diagram of the fingerprint authentication equipment of the gestalt of operation of the 2nd of this invention,

[Drawing 3] It is the functional block diagram of a radio terminal which performs the conventional fingerprint authentication.

[Description of Notations]

1 Electric Power Switch

2 Fingerprint Read Station

3 Fingerprint Registration Section

4 Fingerprint Authentication Section

5 Motion-Control Section

6 Microphone

7 Voiceprint Registration Section

8 Voiceprint Authentication Section

9 Timer Section

10 User Recognition Section

21 Multi-stage Switch

22 Random Number Generation Section

23 Digital Signature Section

24 Key Share Processing Section

25 Encryption Processing Section

[Translation done.]

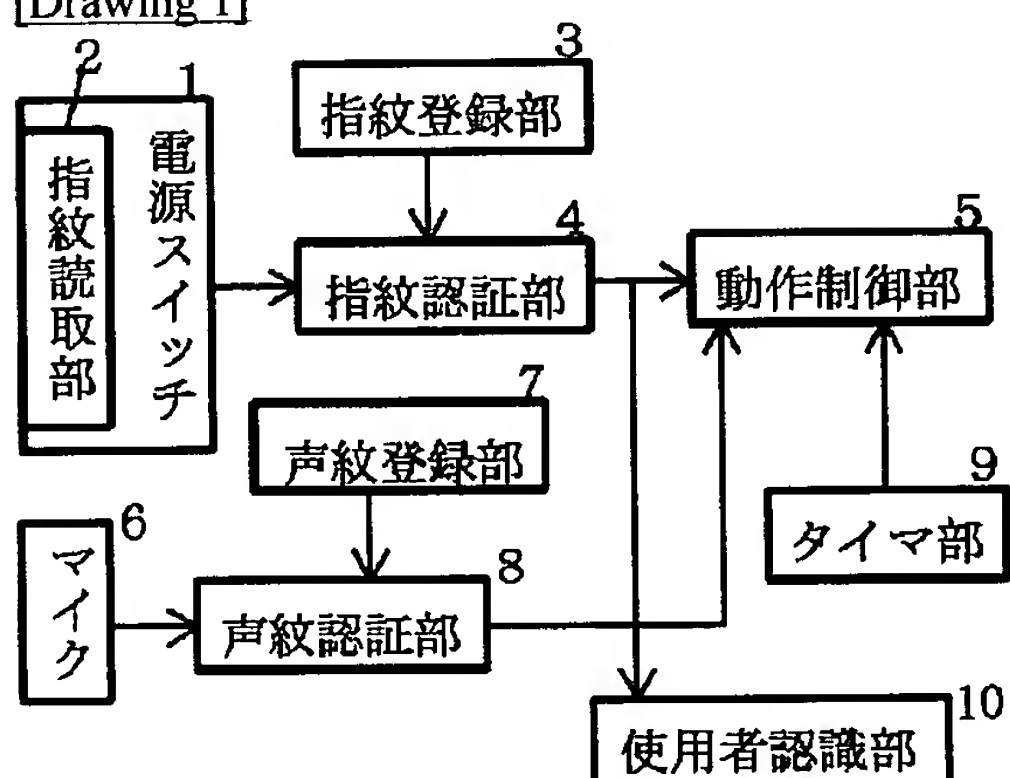
* NOTICES *

Japan Patent Office is not responsible for any damages caused by the use of this translation.

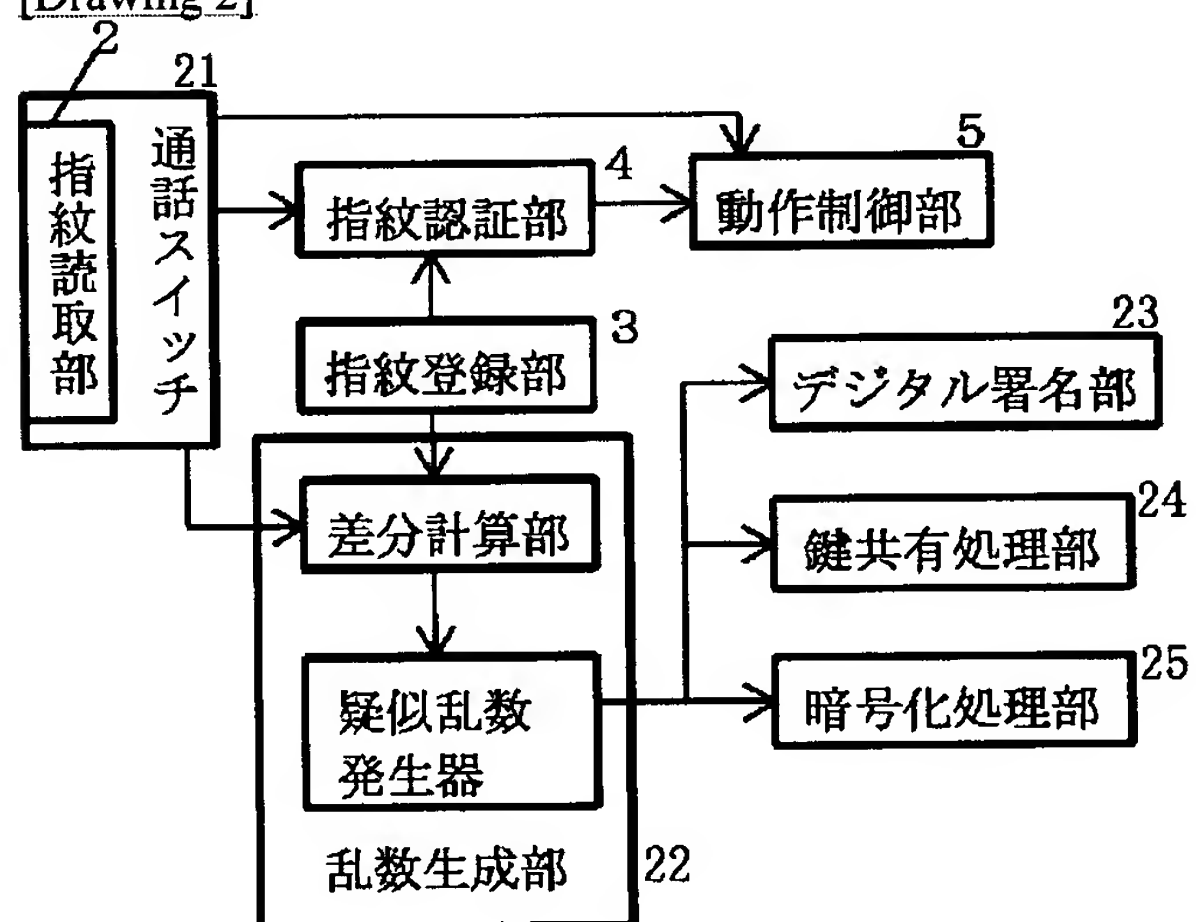
1. This document has been translated by computer. So the translation may not reflect the original precisely.
2. **** shows the word which can not be translated.
3. In the drawings, any words are not translated.

DRAWINGS

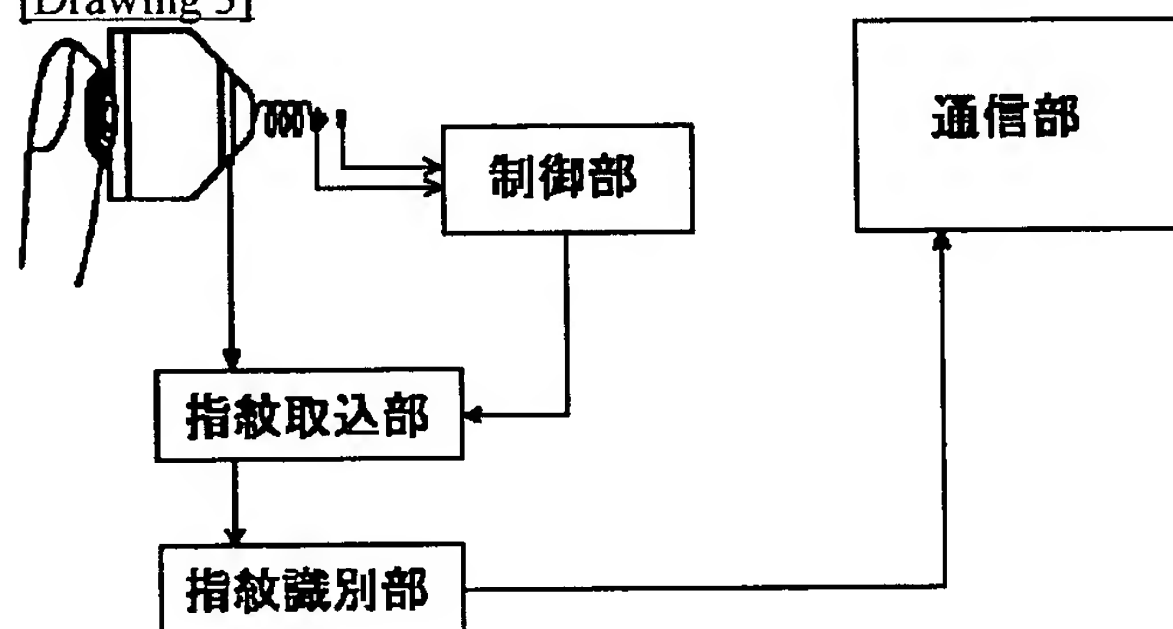
[Drawing 1]



[Drawing 2]



[Drawing 3]



[Translation done.]

(19) 日本国特許庁 (J P)

(12) 特 許 公 報 (B 2)

(11) 特許番号

特許第3258632号

(P3258632)

(45) 発行日 平成14年2月18日 (2002.2.18)

(24) 登録日 平成13年12月7日 (2001.12.7)

(51) Int. Cl. ⁷	識別記号	P I
H 0 4 L 9/32		G 0 6 T 1/00 4 0 0 G
G 0 6 T 1/00	4 0 0	G 0 9 C 1/00 6 5 0 B
G 0 9 C 1/00	6 5 0	H 0 4 L 9/00 6 7 3 D
H 0 4 Q 7/38		H 0 4 B 7/26 1 0 9 S

請求項の数 5 (全 6 頁)

(21) 出願番号	特願平10-335723	(73) 特許権者	597174182 株式会社高度移動通信セキュリティ技術 研究所 神奈川県横浜市港北区新横浜三丁目20番 地8
(22) 出願日	平成10年11月26日 (1998.11.26)	(72) 発明者	安藤 潤 神奈川県横浜市港北区新横浜三丁目20番 地8 株式会社高度移動通信セキュリティ 技術研究所内
(65) 公開番号	特開2000-165378 (P2000-165378A)	(72) 発明者	加藤 武比古 神奈川県横浜市港北区新横浜三丁目20番 地8 株式会社高度移動通信セキュリティ 技術研究所内
(43) 公開日	平成12年6月16日 (2000.6.16)	(74) 代理人	100099254 弁理士 役 昌明 (外1名)
審査請求日	平成11年6月2日 (1999.6.2)		
		審査官	中里 裕正
			最終頁に続く

(54) 【発明の名称】 指紋認証装置

1

(57) 【特許請求の範囲】

【請求項1】 電子機器の電源スイッチまたは動作スイッチに設けた指紋読取部と、複数の人の指紋を登録できる指紋登録部と、前記指紋読取部で読み取った読取指紋データと前記指紋登録部の登録指紋データとを比較する指紋認証部と、前記指紋認証部の比較結果に基づいて前記電子機器を動作させる手段と、前記電子機器の動作開始後一定時間経過したら電源をオフにする手段と、前記指紋認証部の比較結果に基づいて、指紋登録部に登録された人を、前記電子機器を使用した人として認識する手段と、前記登録指紋データと前記読取指紋データとの差分データを求める手段と、前記差分データに基づいて乱数を生成する手段とを具備することを特徴とする指紋認証装置。

【請求項2】 前記乱数を用いてデジタル署名を生成す

2

るとともに相手のデジタル署名を認証する手段を設けたことを特徴とする請求項1記載の指紋認証装置。

【請求項3】 前記乱数を用いて鍵共有処理を行なう手段を設けたことを特徴とする請求項1記載の指紋認証装置。

【請求項4】 前記乱数を用いて公開鍵暗号による暗号化処理を行なう手段を設けたことを特徴とする請求項1記載の指紋認証装置。

【請求項5】 前記通話スイッチを多段スイッチとし、前記通話スイッチの半押し状態において指紋認証と乱数発生を行なう手段と、前記通話スイッチの全押し状態において指紋認証の結果に基づいて前記移動無線端末機を通信可能にする手段とを設けたことを特徴とする請求項1記載の指紋認証装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、移動無線端末機などに用いる指紋認証装置に関し、特に、使用者の指紋に基づいて乱数を発生する指紋認証装置に関する。

【0002】

【従来の技術】従来の指紋認証装置は、機器の電源スイッチを入れてから、指紋認証装置に指を当てて指紋認証を行ない、認証に合格すれば機器が動作するようになっていた。あるいは、機器の電源スイッチは常にオンになっており、指紋認証に合格すれば動作スイッチが有効になり、機器が動作するようになっていた。

【0003】特開平10-51441号公報には、図3に示すような無線通信端末が開示されている。これは、使用者の指紋照合を使用中當時行ない、特定された使用者しか使用することのできない高度なセキュリティ機能を有する無線通信端末である。通信ボタンを押した指の指紋を指紋取込部で使用者指紋として取り込み、指紋識別部で、この使用者指紋を登録指紋と照合して、一致か不一致かを識別する。通信ボタンが押されていることを通信スイッチで検出し、これを条件として通信を可能にする。登録指紋と使用者指紋とが不一致のときには通信部が通信を終了する。

【0004】特開平6-284182号公報には、携帯電話機が開示されている。これは、本来の利用者以外の人に利用させないようにする十分なセキュリティ機能を有し、また、落としたりした場合に、拾った人が容易に本来の利用者に連絡することができる無線式携帯電話機である。セキュリティ制御部は、セキュリティボタン、電源スイッチの操作に応じて、指紋読み取り部、指紋登録部、指紋照合比較部、指紋一時記憶部を制御し、指紋の登録、照合を行なわせ、かつ、セキュリティ状態とセキュリティ解除状態の切換えを行なう。また、緊急通報制御手段は、緊急通報用ボタンが押下される毎に、複数の緊急通報先の中で、優先順位の高い順に、発呼する緊急通報先を切り換え、ディスプレイに緊急通報先を表示し、電話機能部を制御して、緊急通報用電話番号記憶部から読み出した緊急通報先の電話番号へ発呼する。

【0005】特開平5-95329号公報には、携帯電話装置が開示されている。これは、特定の使用者の人体的情報（指紋）を指紋読取部で読み取り、予め記憶しておいた情報と比較して、一致した時に送受信部を動作状態にする携帯電話装置である。指紋の代わりに音声パラメータを比較することもできる。

【0006】特開平10-1984453号公報には、パーソナルコンピュータシステムが開示されている。これは、システムに指センサを搭載することで、パスワード入力を指紋照合に代え、セキュリティ機能の充実をはかる他、使用者個人による環境設定の自動化等、融通性の高い使用法を実現したパーソナルコンピュータシステムである。指センサにより採取された指データをシステムに取り込

み、指データ毎、定義される環境設定データを生成し、データベース（指登録環境設定テーブル）として登録し、指データの入力があったときにデータベースとの比較照合を行ない、その比較照合の結果によって、登録された環境設定情報に従い自動セットアップ操作を行なう。

【0007】

【発明が解決しようとする課題】しかし、従来の装置では、指紋照合により個人を認証するのみであり、指紋データを十分活用していなかった。そのために、多くの装置を使用してセキュリティを高める方法をとるしかなかったため、装置のコストが高くなるという問題があった。また、移動無線端末機の場合、端末装置自体の識別しかできず、使用者がだれであるか識別することができないという問題があった。

【0008】また、移動無線端末機以外の電子機器、例えばコピー機などでは、使用者を認証するために磁気カードを使っており、認証結果を使って課ごとに課金するような管理を行なっているが、磁気カードの紛失や無断借用などによる不正使用を防止することが困難であるという問題があった。

【0009】本発明は、上記従来の問題を解決し、指紋認証によるセキュリティの向上およびそれに伴うステップの削減を目的とする。

【0010】また、電子機器の利用者を指紋により管理して、コピー機などを課ごとに課金できるようにすることを目的とする。

【0011】

【課題を解決するための手段】上記の課題を解決するために、本発明では、指紋認証装置を、電子機器の電源スイッチまたは動作スイッチに設けた指紋読取部と、複数の人の指紋を登録できる指紋登録部と、指紋読取部で読み取った読取指紋データと指紋登録部の登録指紋データとを比較する指紋認証部と、指紋認証部の比較結果に基づいて電子機器を動作させる手段と、電子機器の動作開始後一定時間経過したら電源をオフにする手段と、電子機器を使用した人を認識する手段とを具備する構成とした。このように構成したことにより、認証操作が不要になり、指紋認証をクリアしないと起動・動作せず、電源オン状態でも、一定時間で切れるので、不正使用を防止できるとともに、機器を特定の複数の人で使用でき、機器使用者を識別して表示することができる。

【0012】また、移動無線端末機の通話スイッチに指紋読取部を設けた。このように構成したことにより、認証操作が不要になり、指紋認証をクリアしないと移動無線端末機で通話できず、不正使用を防止できる。

【0013】また、人の声紋を登録する声紋登録部と、送話マイクに入力された音声の入力声紋データと声紋登録部の登録声紋データとを比較して声紋認証を行なう声紋認証部と、声紋認証の結果に基づいて移動無線端末機

5

を通信可能にする手段とを設けた。このように構成したことにより、認証操作が不要になり、声紋認証をもクリアしないと移動無線端末機で通話できず、不正使用を防止できる。

【0014】また、複写機のコピースイッチに指紋読取部を設けた。このように構成したことにより、認証操作が不要になり、指紋認証をクリアしないと複写機で複写できず、不正使用を防止できる。

【0015】また、登録指紋データと読取指紋データとの差分データを求める手段と、差分データに基づいて乱数を生成する手段とを設けた。このように構成したことにより、簡単に乱数が生成できる。

【0016】また、乱数を用いてデジタル署名を生成するとともに相手のデジタル署名を認証する手段を設けた。このように構成したことにより、デジタル署名および相手認証が効率的にできる。

【0017】また、乱数を用いて鍵共有処理を行なう手段を設けた。このように構成したことにより、鍵共有が効率的にできる。

【0018】また、乱数を用いて公開鍵暗号による暗号化処理を行なう手段を設けた。このように構成したことにより、暗号化処理が効率的にできる。

【0019】また、通話スイッチを多段スイッチとし、通話スイッチの半押し状態において指紋認証と乱数発生を行なう手段と、通話スイッチの全押し状態において指紋認証の結果に基づいて移動無線端末機を通信可能にする手段とを設けた。このように構成したことにより、1つのスイッチで認証と通話の機能を選択できる。

【0020】

【発明の実施の形態】本発明の請求項1に記載した発明は、電子機器の電源スイッチまたは動作スイッチに設けた指紋読取部と、複数の人の指紋を登録できる指紋登録部と、前記指紋読取部で読み取った読取指紋データと前記指紋登録部の登録指紋データとを比較する指紋認証部と、前記指紋認証部の比較結果に基づいて前記電子機器を動作させる手段と、前記電子機器の動作開始後一定時間経過したら電源をオフにする手段と、前記指紋認証部の比較結果に基づいて、指紋登録部に登録された人を、前記電子機器を使用した人として認識する手段と、前記登録指紋データと前記読取指紋データとの差分データを求める手段と、前記差分データに基づいて乱数を生成する手段とを具備する指紋認証装置であり、スイッチ押下時に指紋認証を行ない、動作を一定時間に制限して不正使用を防止するとともに、指紋の雑音成分を利用して乱数を発生するという作用を有する。

【0021】本発明の請求項2記載の発明は、請求項1記載の指紋認証装置において、前記乱数を用いてデジタル署名を生成するとともに相手のデジタル署名を認証する手段を設けたものであり、デジタル署名および相手認証を簡単化するという作用を有する。

6

【0022】本発明の請求項3記載の発明は、請求項1記載の指紋認証装置において、前記乱数を用いて鍵共有処理を行なう手段を設けたものであり、鍵共有処理を簡単化するという作用を有する。

【0023】本発明の請求項4記載の発明は、請求項1記載の指紋認証装置において、前記乱数を用いて公開鍵暗号による暗号化処理を行なう手段を設けたものであり、公開鍵暗号による暗号化処理を簡単化するという作用を有する。

【0024】本発明の請求項5記載の発明は、請求項1記載の指紋認証装置において、前記通話スイッチを多段スイッチとし、前記通話スイッチの半押し状態において指紋認証と乱数発生を行なう手段と、前記通話スイッチの全押し状態において指紋認証の結果に基づいて前記移動無線端末機を通信可能にする手段とを設けたものであり、1つのスイッチで認証・乱数発生と通話を兼用するという作用を有する。

【0025】

【0026】

【0027】

【0028】

【0029】以下、本発明の実施の形態について、図1と図2を参照しながら詳細に説明する。

【0030】（第1の実施の形態）本発明の第1の実施の形態は、移動無線端末機の電源スイッチに指紋読取部を設け、複数の人の指紋を指紋登録部に登録し、指紋読取部で読み取った読取指紋データと指紋登録部の登録指紋データとを指紋認証部で比較し、指紋認証部の比較結果に基づいて使用者を認識するとともに移動無線端末機を動作させ、入力音声の声紋データと登録してある声紋データとを比較した結果に基づいて移動無線端末機を通信可能にし、移動無線端末機の動作開始後一定時間経過したら電源をオフにする指紋認証装置である。

【0031】図1は、本発明の第1の実施の形態の指紋認証装置の機能ブロック図である。図1において、電源スイッチ1は、移動無線端末機の電源スイッチである。指紋読取部2は、使用者の指紋を読み取る手段である。指紋登録部3は、複数の人の指紋を登録した記憶装置である。指紋認証部4は、指紋読取部2で読み取った読取指紋データと指紋登録部3の登録指紋データとを比較する手段である。動作制御部5は、指紋認証部4の比較結果に基づいて移動無線端末機を動作させる手段である。マイク6は、移動無線端末機の送話用マイクである。声紋登録部7は、複数の使用者の声紋を登録した記憶装置である。声紋認証部8は、入力音声の声紋データと登録声紋データとを比較して声紋認証を行なう手段である。タイマ部9は、移動無線端末機の動作開始後一定時間経過したら電源をオフにする手段である。使用者認識部10は、移動無線端末機を使用した人を認識する手段である。

【0032】上記のように構成された本発明の第1の実施の形態の指紋認証装置の動作を説明する。

【0033】移動無線端末機の電源スイッチ1に設けた指紋読取部2で、指紋を読み取る。複数の人の指紋を指紋登録部3に登録しておく。指紋読取部2で読み取った読取指紋データと指紋登録部3の登録指紋データとを指紋認証部4で比較する。使用者認識部10で、指紋認証結果に従って、移動無線端末機を使用した人を認識する。動作制御部5は、指紋認証部4の比較結果に基づいて移動無線端末機を動作させるが、まだ、通信可能にはしない。

【0034】複数の人の声紋を声紋登録部7に登録しておく。マイク6に入力された音声の入力声紋データと声紋登録部7の登録声紋データとを声紋認証部8で比較して、声紋認証を行なう。声紋認証の結果に基づいて移動無線端末機を通信可能にする。指紋認証と併用して声紋認証を行なって、よりセキュリティを高める。複数の人の指紋と声紋を登録することで、移動無線端末機を複数の人で使用することができる。

【0035】移動無線端末機の動作開始後一定時間経過したら、タイマ部9により電源をオフにする。認証合格して起動しても、タイマ部9により一定時間で電源を切るので、動作状態のままでの紛失や盗難の場合でも、不正使用を防止できる。

【0036】上記のように、本発明の第1の実施の形態では、指紋認証装置を、移動無線端末機の電源スイッチに指紋認証部を設け、スイッチと指紋認証を連動させて、指紋認証により動作させる構成としたので、スイッチを押すという操作だけで指紋認証ができ、セキュリティを高めることができる。

【0037】なお、本実施の形態では指紋認証装置を移動無線端末機に設けたものを説明したが、複写機の電源スイッチかコピースイッチに指紋読取部を設けて、複写機の利用者を限定することもできる。このようにして、磁気カードを使用しなくても課ごとに課金することができる。不正使用の防止とともに、課金管理を容易かつ厳密に行なうことができる。

【0038】（第2の実施の形態）本発明の第2の実施の形態は、移動無線端末機に多段スイッチを用いて、全押しならば通話を行ない、半押しならば認証・乱数発生を行ない、登録済み指紋と認識した指紋の差から乱数を生成し、乱数を用いてデジタル署名および相手認証を行ない、乱数を用いて鍵共有を行ない、乱数を用いて公開鍵暗号による暗号化を行なう指紋認証装置である。

【0039】図2は、本発明の第2の実施の形態の指紋認証装置の機能ブロック図である。図2において、通話スイッチ21は、半押し状態において指紋認証と乱数発生を行ない、全押し状態において指紋認証の結果に基づいて移動無線端末機を通信可能にする多段スイッチである。乱数生成部22は、登録指紋データと読取指紋データ

との差分データを求め、差分データに基づいて乱数を生成する手段である。デジタル署名部23は、乱数を用いてデジタル署名を生成するとともに相手のデジタル署名を認証する手段である。鍵共有処理部24は、乱数を用いて鍵共有処理を行なう手段である。暗号化処理部25は、乱数を用いて公開鍵暗号による暗号化処理を行なう手段である。

【0040】上記のように構成された本発明の第2の実施の形態の指紋認証装置の動作を説明する。移動無線端末機が多段通話スイッチ21の半押し状態において、指紋認証と乱数発生を行ない、通話スイッチ21の全押し状態において、指紋認証の結果に基づいて移動無線端末機を通信可能にする。

【0041】乱数生成部22において、登録指紋データと読取指紋データとの指紋の位置、範囲、角度、データ量などの差分データを求め、差分データを疑似乱数発生器のシードとして乱数を生成する。デジタル署名部23において、乱数を用いてデジタル署名を生成するとともに、相手のデジタル署名を認証する。鍵共有処理部24では、乱数を用いて鍵共有処理を行なう。暗号化処理部25では、乱数を用いて公開鍵暗号による暗号化処理を行なう。ElGamal署名やDSA署名、楕円ElGamal署名、楕円DSA署名、D-H鍵共有、楕円DH鍵共有、ElGamal暗号、楕円ElGamal暗号には乱数が必要であるので、指紋データから求めた乱数を利用して、簡単にデジタル署名の生成などを行なうことができる。

【0042】上記のように、本発明の第2の実施の形態では、指紋認証装置を、多段スイッチを用いて、全押しならば通話を行ない、半押しならば認証・乱数発生を行ない、登録済み指紋と認識した指紋の差から乱数を生成し、乱数を用いて、デジタル署名および相手認証や、鍵共有や、公開鍵暗号による暗号化を行なう構成としたので、指紋から生成した乱数を利用して各種の暗号処理を簡単に行なうことができる。

【0043】

【発明の効果】以上のように、本発明では、指紋認証装置を、電子機器の電源スイッチまたは動作スイッチに設けた指紋読取部と、複数の人の指紋を登録できる指紋登録部と、指紋読取部で読み取った読取指紋データと指紋登録部の登録指紋データとを比較する指紋認証部と、指紋認証部の比較結果に基づいて電子機器を動作させる手段と、電子機器の動作開始後一定時間経過したら電源をオフにする手段と、電子機器を使用した人を認識する手段とを具備する構成としたので、1操作で指紋認証をして、端末を使用する人を識別することができるとともに、動作状態のままでの紛失や盗難の場合でも、不正使用を防止できるという効果が得られる。

【0044】また、移動無線端末機の通話スイッチに指紋認証部を設け、スイッチと指紋認証を連動させる構成としたので、通話スイッチ操作で指紋認証をして、移動

無線端末機不正使用を防止できるという効果を得られる。

【0045】また、人の声紋を登録する声紋登録部と、送話マイクに入力された音声の入力声紋データと声紋登録部の登録声紋データとを比較して声紋認証を行なう声紋認証部と、声紋認証の結果に基づいて移動無線端末機を通信可能にする手段とを設けたので、よりセキュリティを高めることができるという効果を得られる。

【0046】また、複写機のコピースイッチに指紋認証部を設けたので、コピースイッチの操作で指紋認証をして、スイッチと指紋認証を連動させ、複写機不正使用を防止できるとともに、課ごとの課金などが容易にできるという効果を得られる。

【0047】また、登録指紋データと読取指紋データとの差分データを求める手段と、差分データに基づいて乱数を生成する手段とを設けたので、指紋の雑音成分から簡単に乱数を生成できるという効果を得られる。

【0048】また、乱数を用いてデジタル署名を生成するとともに相手のデジタル署名を認証する手段を設けたので、乱数から簡単にデジタル署名および相手認証ができるという効果を得られる。

【0049】また、乱数を用いて鍵共有処理を行なう手段を設けたので、乱数から簡単に鍵共有を行なうことができるという効果を得られる。

【0050】また、乱数を用いて公開鍵暗号による暗号化処理を行なう手段を設けたので、乱数から簡単に公開鍵暗号による暗号化処理を行なうことができるという効果を得られる。

【0051】また、通話スイッチを多段スイッチとし、*

*通話スイッチの半押し状態において指紋認証と乱数発生を行なう手段と、通話スイッチの全押し状態において指紋認証の結果に基づいて移動無線端末機を通信可能にする手段とを設けたので、1つのスイッチで認証・乱数発生と通話が簡単できるという効果を得られる。

【図面の簡単な説明】

【図1】本発明の第1の実施の形態の指紋認証装置の機能ブロック図。

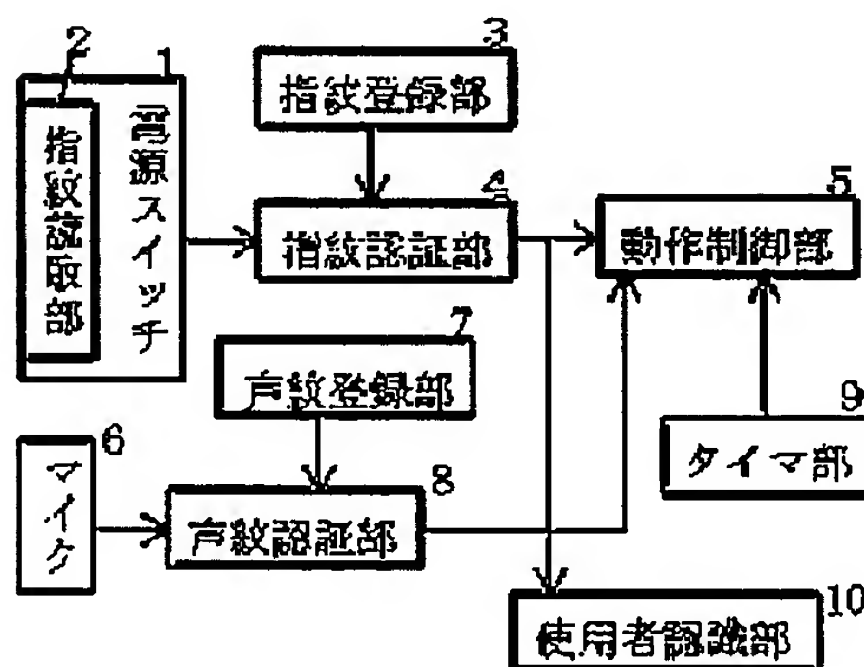
【図2】本発明の第2の実施の形態の指紋認証装置の機能ブロック図。

【図3】従来の指紋認証を行なう無線通信端末の機能ブロック図である。

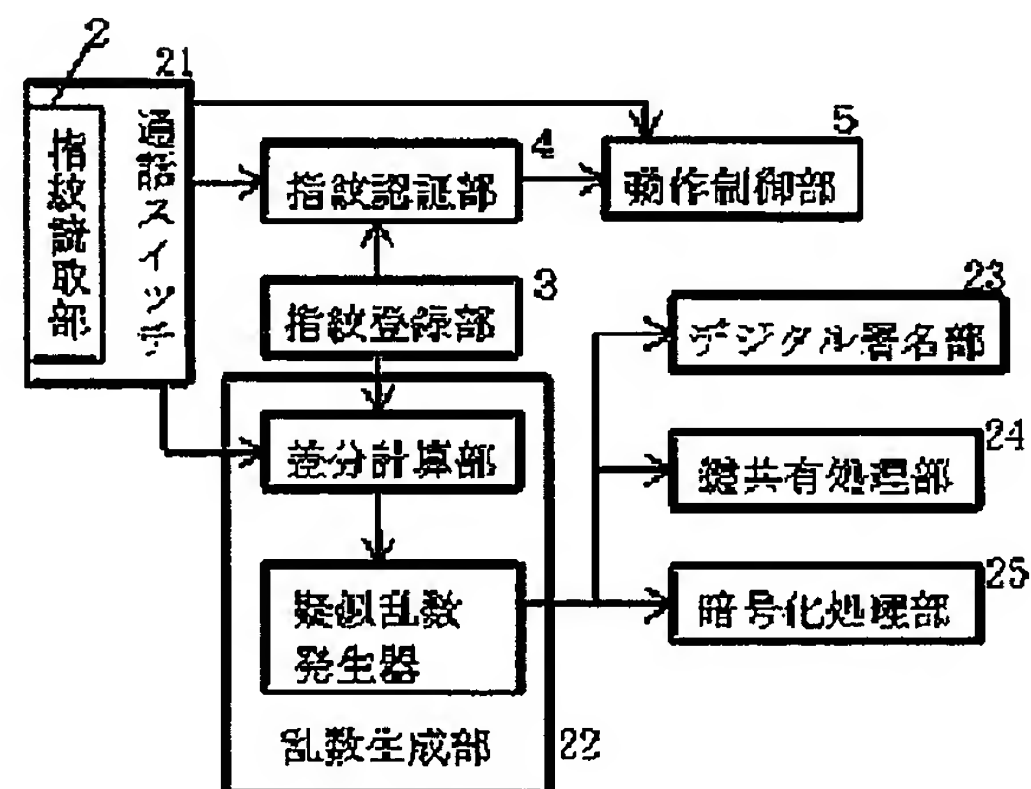
【符号の説明】

- 1 電源スイッチ
- 2 指紋読取部
- 3 指紋登録部
- 4 指紋認証部
- 5 動作制御部
- 6 マイク
- 7 声紋登録部
- 8 声紋認証部
- 9 タイマ部
- 10 使用者認識部
- 21 多段スイッチ
- 22 乱数生成部
- 23 デジタル署名部
- 24 鍵共有処理部
- 25 暗号化処理部

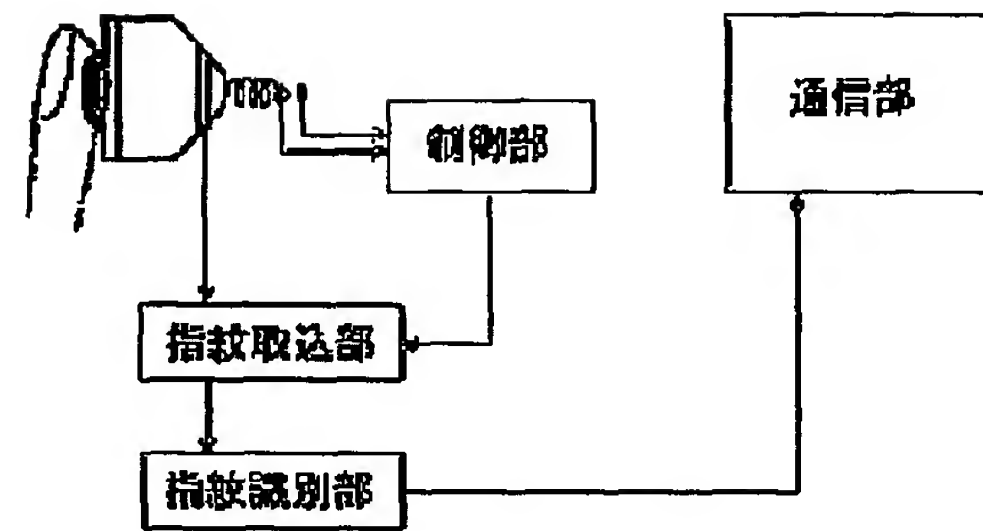
【図1】



【図2】



【図3】



フロントページの続き

(72)発明者 松崎 なつめ

神奈川県横浜市港北区新横浜三丁目20番
地8 株式会社高度移動通信セキュリテ
ィ技術研究所内

(72)発明者 伊藤 哲

神奈川県横浜市港北区新横浜三丁目20番
地8 株式会社高度移動通信セキュリテ
ィ技術研究所内

(56)参考文献 特開 平7-129049(JP,A)
特開 昭62-138781(JP,A)
特開 平10-51441(JP,A)
特開 平10-51349(JP,A)
特開 平4-348408(JP,A)
特表 平10-505474(JP,A)

(58)調査した分野(Int.Cl.⁷, DB名)

H04L 9/32
G06T 1/00 400
G09C 1/00 650
H04Q 7/38